STATE of ARIZONA

Government **I**nformation **T**echnology **A**gency	**Statewide** **POLICY** **P140**	**TITLE: Web Conferencing** **Effective Date: September 14, 2007**

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (A.R.S. § 41-3504(A (1))), including, the formulation of policies to effectuate the purposes of the agency (A.R.S. § 41-3504(A (13))).

2. PURPOSE

The purpose of this policy is to identify Web conferencing (WC) best practice activities for state communications and collaboration with other state agencies, counties, cities, local governments, federal government, and third party organizations. The opportunity to save time and expense on behalf of state personnel by utilizing Web conferencing for virtual classrooms and meetings is compelling, productive, efficient, and effective for state government.

3. SCOPE

A Budget Unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending, or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents, the community college districts and the legislative and judicial branches (A.R.S. § 41-3501(2)).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. POLICY

Web conferencing systems are becoming more and more integrated with respect to audio, video, and messaging with real-time communications over networks and the Internet supporting both conference settings and presentation formats. State agencies should utilize client/server Web conferencing systems as a convenience for agency personnel who participate in meetings when attendance is an issue either at various physical locations, or the high cost of business travel, or of the health or security restrictions on behalf of state personnel. The following policy statements address best practices for state government personnel when preparing and conducting a Web Conference.

4.1. **Conferencing Via the Web**
Information exchange, presentations, and group discussions during an online Web conference can be among the most sensitive information for the state and its participants. Therefore, it is important to start with the following basic conference fundamentals.

4.1.1 **Registration –** The purpose of registration is to ensure that the correct participants receive the information they need to participate in the conference. At a minimum, the registration invitation and/or email calendar entry should include date and time, a Web URL, a phone number to call in for the audio portion (if separate audio circuit), and ID/password to provide access to the Web conference.

A. Verify the invitation list to ensure it is correct and up-to-date (intended audience), and does not include generic email addresses like gitastaff@azgita.gov unless specifically intended.

B. If available, use secure email (i.e., Secure Socket Layer, SSL) to send registration and confirmation information with the "DO NOT FORWARD" feature selected.

C. For regular or recurring meetings periodically change the user ID and password (as per password PSP standards). For confidential meetings change the password prior to every meeting.

4.1.2 **Confirmation** – When participants have confirmed attendance either by phone, letter or email, send a secure registration confirmation either by letter and/or email to confirm their attendance.

4.1.3 **Conference Transmission** – To reduce the risk of presentation and document content being intercepted during transmission over the Internet, most Web conferencing systems use the Secure Socket Layer (SSL) protocol for encrypting content as it passes among participants and host client/server devices. Ensure that this security feature is enabled for conferencing.

A. When videoconferencing, position cameras so they cannot transmit more than they should; for example, whiteboards with content from previous meetings, personal artifacts, nonparticipating employees or visitors. Your conference location should look professional in representing the State of Arizona.

B. Cameras, microphones or speaker phones should be turned on only at the start of the conference and immediately turned off at the conclusion of the meeting.

4.1.4 **Conference Identification** – When the conference has started, the moderator must identify all participants and verify that they are authorized to participate in the meeting.

A. All participants can be issued a unique personal identification number (PINs) when using the phone or audio bridge feature of the Web conference rather than one PIN for everyone. This facilitates

better identification and security for the Web conference. In any case, where possible, individuals attending on the web should sign in as part of a record of their attendance.

B. Audio bridging has additional features that allow the moderator to exclude anonymous participants from the meeting.

C. The moderator should tell all participants that the conference cannot be overheard or seen by unauthorized individuals in keeping the trust and integrity of the meeting; discourage the use of speakerphones except in closed rooms.

4.1.5 **Web Conference Technician** - A trained individual within the agency, familiar with the Web conference system should be present for initial conference preparations, startup, transmission, and shutdown. Such an individual can remedy technical problems and eliminate delays and frustrations for the conference. If necessary, the individual can be dismissed just after transmission begins and reenter the conference at its conclusion to shutdown the system.

4.2. Privacy Issues with Web Conferencing

When Web conferencing presentations are without video, the moderator and participants are unable to see if others are paying attention or have left the conference, especially if the conference is spread across several physical locations. Moderators and presenters at times need this type of information to determine whether they should speed up delivery, liven up their style, or verify if the topics being discussed are useful. Moderators and presenters can obtain feedback in the following ways:

4.2.1. Ask participants directly if the material is interesting;

4.2.2. Conduct a survey or a poll;

4.2.3. Implement Web conference products that provide “attentiveness monitoring” and/or “participation meters”;

4.2.4. The agency hosting the conference should announce beforehand to all participants that such monitoring/meters will be enabled to avoid privacy concerns and issues. Any perceived invasion of privacy is a serious breach of trust;

4.2.5. State agencies with Web conference systems that have monitoring/meter features enabled should automatically inform participants that they are in use and some aspects of behavior will be reported to meeting moderators/presenters, and should offer participants a chance to opt-out.

4.3. Web Conferencing Tools and Features*

Web conferencing enables a group of individuals to interact in real time via the Web with the ability for a moderator or presenter to show and demonstrate a variety of media and information to a wide audience. Web conference systems rely on a variety of interfaces in that a client device(s) provides the visual interface, a conventional telephone (or IP phone) provides the voice, and Instant

Messaging (IM) or Chat provides text messaging among participants. Web conference technologies should contain the following tools and features:

4.3.1. Document-centric conferencing;

4.3.2. Slide show presentations;

4.3.3. Recorded audio with presentations;

4.3.4. Screen and document sharing;

4.3.5. Shared whiteboards with capture;

4.3.6. Polling or testing mechanisms;

4.3.7. Archiving, search and replay of conference proceedings;

4.3.8. Integration with group videoconferencing systems;

4.3.9. Bidirectional application sharing and remote control.

4.3.10. Instant Messaging (IM) and Chat and text delivery;

4.3.11. The moderator or conference leader may enable:

- File-transfer and application download capabilities
- Shared file printing capability

4.3.12. Voice and video over Internet Protocol (AzNet - VoIP) within Web conferences;

4.3.13. A recording feature, for later use or archiving of the conference.

4.3.14. User/technical interfaces and development models (such as Portals, Ajax, and Rich Internet Clients);

* The above tools and features are recommendations for a robust Web conference system; it is the Budget Unit's discretion to enable any of the above tools and features based on the configuration of the system.

4.4. **Security Issues for Web Conferencing**

Web conference hosts and participants should assess the security needs of their meetings. Some online meetings may be considered as "public meetings" and have fewer security concerns than that of a "Closed Door Session" that may be highly sensitive in nature. Nevertheless, networks and supporting security practices must comply with the state's current infrastructure as well as statewide IT policies and standards.

4.4.1. **Statewide Network and Security Foundation** – The AzNET program managed by the Telecommunications Program Office (TPO) of ADOA is a well managed robust network with security tools and methods in place to meet the needs of state government for Web conferencing. Such tools and methods include network perimeter security, tiered firewalls, end-point security, DMZ security, intrusion detection & prevention, email protection, encryption and filtering, web-content filtering, strong authentication services, Defense in Depth layered security services, and Multi-Protocol label Switching (MPLS).

4.4.2. **Budget Unit Network and Security Foundation** - Budget units maintaining their own existing networks and security tools shall be compatible with the state's AzNET program in addition to compliance with the statewide P710 Network Architecture policy, S710 Network Infrastructure Standard, P800 IT Security Policy, and the S830 Network Security Standard.

4.4.3. **Object Security –** Many Web conferences will discuss and view shared documents or presentations which may have specific security concerns:

A. Files, documents, and presentations that are viewed or shared during conferences that are sensitive in nature and not for distribution, are impossible to keep confidential. There is no practical way to prevent participants from using screen capturing software tools or the <print screen> key to either print, file save, or record images off the screen. Therefore, it is best not to display extremely sensitive documents during a Web conference.

B. If the Web Conference requires participants to load presentations or documents on a hosted server, then at the conclusion of the meeting delete the presentations and documents manually or use an automatic purge setting on the system.

C. Some Web conferencing systems allow participants to automatically transfer files or download information during a conference. Turn off these features if participants are not allowed to do this during a conference.

4.4.4. **Physical Security** – Often times, the simplest actions or lack of preparation for a conference can create security and trust issues, whether perceived or real. For example: Room preparation and lack thereof, open windows with visual traffic in the background, whiteboards with unfamiliar or sensitive content, cameras viewing irrelevant points of interests, and turned on microphones that provide unfamiliar sounds, noises, traffic, or unknown participants. Anything viewed or heard as suspicious will generate mistrust in a Web conference.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-1335 ((A (6 & 7))), "Budget Unit Information."
6.2. A. R. S. § 41-1346 (A), "Records Management Program."
6.3. A. R. S. § 41-1461, "Definitions."
6.4. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.5. A. R. S. § 41-3501, "Definitions."
6.6. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.7. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.8. A. R. S. § 44-7041, "Governmental Electronic Records."

6.9. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.10. Statewide Policy P100, Information Technology.
6.11. Statewide Policy P340, Project Investment Justification (PIJ).
6.12. Statewide Policy P710, Network Architecture.
6.13. Statewide Policy P720, Platform Architecture.
6.14. Statewide Policy P730, Software Architecture.
6.15. Statewide Policy P740, Data/Information Architecture.
6.16. Statewide Policy P800, IT Security.

7. ATTACHMENTS

None.